

# A Study of Original and Tempered Images for Real-Fake Image

**Prof. Vikas Singhal**

Department - Information Technology  
Greater Noida Institute of Technology (Engineering Institute)  
Gautam Buddh Nagar, India  
[vikassinghal75@gmail.com](mailto:vikassinghal75@gmail.com)

**Dr. Shivani Dubey**

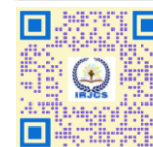
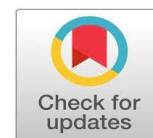
Department - Information Technology  
Greater Noida Institute of Technology (Engineering Institute)  
Gautam Buddh Nagar, India  
[dubey.shivani@gmail.com](mailto:dubey.shivani@gmail.com)

**Dr. Pankaj Gupta**

Department - Information Technology  
Greater Noida Institute of Technology (Engineering Institute)  
Gautam Buddh Nagar, India  
[drpkg03@gmail.com](mailto:drpkg03@gmail.com)

**Dinesh Mishra**

Department - Information Technology  
Greater Noida Institute of Technology (Engineering Institute)  
Gautam Buddh Nagar, India



## Publication History

Manuscript Reference No: IJIRAE/RS/Vol.11/Issue01/JAAE10094

Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRAE/RS/Vol.11/Issue01/JAAE10094

Received: 03, January 2024 | Revised: 10, January 2024 | Accepted: 19, January 2024 | Published Online: 24, January 2024

<https://www.ijirae.com/volumes/Vol11/iss-01/03/JAAE10094.pdf>

**Article Citation:** Vikas, Shivani, Pankaj, Dinesh (2024). A Study of Original and Tempered Images for Real-Fake Image. IJIRAE::International Journal of Innovative Research in Advanced Engineering, Volume 11, Issue 01 of 2024 pages 16-21

**Doi:** <https://doi.org/10.26562/ijirae.2024.v11i01.03>

**BibTeX** [Vikas2024@Study](mailto:Vikas2024@Study)

**Academic Editor-Chief:** Dr. A. Arul Lawrence Selvakumar, AM Publications, India



Copyright: ©2024 This is an open access article distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited

**Abstract:** The widespread use of image editing technologies in the digital age has raised concerns about the authenticity of visual content. This study delves into the field of image forensics, specifically analyzing original and tempered photos to determine their graphical behavior. The major goal is to develop solid algorithms for distinguishing between authentic and fraudulent photos based on an in-depth assessment of their visual properties. The study makes use of a large data collection that includes both original and manipulated photographs from a variety of sources and contexts. To reveal small differences between authentic and modified pictures, image processing techniques such as noise analysis, color profile investigation, and geometric feature extraction are used. Machine learning algorithms are critical in automating the analysis process and increasing the efficiency and scalability of the proposed methodology. Picture security is an issue for every company that employs digital images. Suspect data has long been used in forensics and public safety pictures, images from crime scenes, biometric photos, and other types of images. In this discipline, the usage of digital photographs has increased dramatically with the advancement of digital imaging. Digital image processing has made picture manipulation easier, but it has also aided in the development of several novel techniques in forensic investigation. Digital picture authenticity is becoming an issue due to the public availability of several programs for cropping and manipulating images. It serves as compelling evidence in many different types of crimes with a variety of purposes. This development is picture processing or edits of two are also simplifies and editing photos. The most typical kinds of Conducted.

## I. INTRODUCTION

The wide spread use of image editing technologies in the digital age has raised concerns about the authenticity of visual content. This study delves into the field of image forensics, specifically analyzing original and tempered photos to determine their graphical behavior. The major goal is to develop solid algorithms for distinguishing between authentic and fraudulent photos based on an in-depth assessment of the visual properties. The study makes use of a large data collection that includes both original and manipulated photographs from a variety of sources and contexts. To reveal small differences between authentic and modified pictures, image processing techniques such as noise analysis, color profile investigation, and geometric feature extraction are used.

Machine learning algorithms are critical in automating the analysis process and increasing the efficiency and scalability of the proposed methodology. Human inspection has been used in traditional picture forensics. These methods can provide precise detection and superior analysis, but they usually take a long time and a lot of effort from people.



**Fig1::** Doctor's photo of British soldiers pointing guns at Iraqis.

Automated content integrity verification has become necessary since the volume of doctored photos that are shared online every day has beyond the capacity of human inspection. Automated algorithms not only expedite verification operations but also supplement human examination for alterations that are imperceptible to the human eye. Technically speaking, a number of issues may be characterized at several levels. Resizing, cropping, color correction or more sophisticated manipulations like content insertion or removal. Detecting these operations helps in understanding how an image has been altered



**Fig2:** Former just a posed alongside actress Jane Fonda.

This image level or binary decision, detection of tampering operation, location of suspicious region, or explanations of alteration. There are several new methods for manipulating photos. For example, this image has been altered by binary authenticity decision making at this photo level (classification).

- It shows inconsistent lighting: manipulation explanation (explanation)
- Added: Falsification of credentials (identification)
- The location of the suspicious spot is where the actress is spliced into the fore ground.

### 1.1. Binary decision making at the image level:

This involves making a binary (yes/no) decision about the authenticity of an entire image. It typically means determining whether an image has been manipulated or tampered with. This decision is based on various forensic techniques that analyze in consistencies, artifacts, or a anomalies in the image data.

### **1.2. Tampering operation identification:**

Tampering operation identification involves recognizing specific operations or manipulations that have been applied to an image.

### **1.3. Suspicious area localization:**

After determining that an image has been tampered with, the next step is to identify the specific regions or areas within the image where the manipulation has occurred. Suspicious area localization aims to pin point the locations where changes or alterations have been made. Analyzing pixel-level variations, in consistencies in lighting or color, and other artifacts that may indicate tampering

### **1.3. Manipulation Explanation:**

Once suspicious areas are identified, the goal is to provide an explanation for the detected manipulation. This involves describing the nature of the tampering operation, such as whether it's a copy-paste operation, image splicing, or other forms of digital manipulation. Understanding the manipulation helps in assessing the credibility and trust worthiness of the image.

## **2. LITERATURE REVIEW**

[1] In this thesis of Jessie Yu-Feng Hsu, Initially, we introduce a completely automated consistency checking algorithm designed to identify splicing with arbitrary shapes. Part of which is the main function of the camera that converts the input radiation into the output image. First, the test image is divided into separate regions. Local plan a irradiance point geometric invariants (LPIP) are used to estimate a CRF for a field. A statistical number is fed into the local image and CRF-based matching to determine whether the boundary between two regions is real or discrete. These phases cores are summed to determine image phase accuracy. Evaluation of two datasets showed good results with 70% sensitivity and 70% recall.

[2] Double JPEG artifacts in multispectral images are often used to identify and analyze local images such as paintings. In this article, we go one step further and propose an end-to-end solution that can identify and find different regions as well as distinguish regions from the different image of the donor. Assuming that both the added region and the background image are double JPEG compressed, we use the local estimate of the main quantization matrix to distinguish the region between different ones.

[3] Image security is a concern for Any business that uses digital photography. Suspect photographs have long been used by forensics and other images. With the development of digital surveying and mapping, the use of digital images in this field has increased significantly. Digital image processing facilitates image manipulation and also supports the development of many new technologies in drug forensic research. The availability of digital images is now an issue, as various screenshot image processing programs are publicly available. It is used as reliable evidence in many crimes and as information for various purposes. Developing image processing and editing software to be creative and editing software has made creating and modifying photos easier and more accessible.

## **III. OBJECTIVES**

The study investigates the effect of popular picture tampering tactics, such as resizing, compression, and content alteration, on image graphical behavior. The work at tempts to establish a deeper understanding of the tell tale indications that can be used for accurate real-fake image classification by detecting the unique finger prints left by these alterations. Furthermore, the inquiry digs into the ethical aspects and societal effects of picture tampering, recognizing the potential for disinformation and misuse that can result from the dissemination of modified visuals. This study's findings have important implications for the development of effective image authentication systems and contribute to the continuing debate about digital trust and visual integrity in the information age

## **IV.METHODOLOGIES**

We use the current approaches as baselines to address the first three research questions, and then we suggest a novel approach to make up for the draw backs with the baselines. then we suggest a novel approach to make up for the we proposed.

### **RQ1**

We want to be present all over the world to expose fake products of fake photos. Our global discovery learns to distinguish fake images from real images and makes it impossible to detect fake images in the open world. We use two different methods: visual-only search and hybrid search. Imageonly detection is in the same spirit as previous work [44] which confirmed the effectiveness of simple CNN in distinguishing fake and real images of GANs. In this work, we consider the most complex and realistic case where we train a simple CNN on fake images generated by only on and then train from unknown standards to evaluate it. Hybrid detection is a new research method in which important articles are combined in learning.

We leverage the CLIP image and text encoder [30] and combine the two embeddings to train the true/false binary classifier. During testing, if the native text of the image is not available, we use BLIP[18] to generate captions for us and then go to the hybrid search and feed the image and text.

## RQ2

We propose using two methods similar to RQ1 to ensure that fake images from different models have different fingerprints. Unlike RQ1, in this phase our multispecies labels learned fake images from different models, one for each label. The image-only feature uses only images, while the composite feature combines images with text. Unlike RQ1 and RQ2,

## RQ3

Focuses on the linguistic modality. To address these inquiries, we purpose the detectors previously trained. More specifically, we conduct a thorough evaluation from two linguistic perspectives: semantic analysis and structural analysis. In this for me, we employ two distinct topic extraction methodologies to scrutinize this influence of topics on this authenticity of synthetic images. Both methods enable us to conclude that prompts describing "person" yield more realistic images. For sentence analysis, we explore the effects of prompt captions based on sentence length and the percentage of nouns in the sentence, respectively. Empirical results reveal that a length between 25 and 75 is optimal for generating highly authentic fake images, while the proportion of nouns in sentences has no bearing on authenticity.

Our insights can assist developers and researchers using the text-to-image diffusion model in producing improved synthetic images, further aiding the community in understanding the inherent characteristics of these images and designing methods with enhanced detection capabilities. Primary Discoveries: The overarching findings and responses to research questions can be succinctly outlined as follows.

## V. DISCOVERY

Different propagation models share artifacts. In addition, integration of information into hybrid search improved the ability to identify these artifacts, improving performance especially when encountering fake images in the open world. Different diffusion models create fingerprints with their images, allowing us to assign fake images to backgrounds. We continue to see these unique fingerprints using images generated from the frequencies demonstrated by Zhang et al.; atmospheric models tend to produce less realistic images. And instructions. Additionally, understanding the latest advances in image forensics is crucial to improving the outcomes of fraud investigations. The number of pictures is 200 and the size is 512\*512 G. (The set of images is very small). When the number of individual tests was reduced, the proposed method outperformed the existing method with an F-score of 90%. Bundy et al. [12] We only accept images from the D0 list. The file consists of 50 full images, is only interpretation proof, and achieves an accuracy of approximately 65%. The second file contains more than 10,000 images with geometric shapes and effects. The accuracy of the information used in this document is approximately 70%. The third file contains many aerial photographs. Only 100 image descriptions were selected for testing. The method achieves accuracy of approximately 90 % of third

Discovery party data (image processing data). (IIMD). Cozzolino et al. [13] developed a new algorithm to detect blind image fusion; these features of the spliced regions are evaluated arbitrarily and distinguished by auto encoder based modeling and hate. Preliminary findings are promising not only in ideal conditions but also in non-ideal conditions. But when success is achieved later, the authors of this work propose a method to place the image link against the mesh communication network (FCN). First, we evaluated a label-only trained FCN task (SFCN). Even while SFCN sometimes performs better than earlier techniques, it still yields subpar regional outcomes.



Fig3: copy move forgery image

Thus, for different training tasks, we suggest using multi-task FCN(MFCN) with two branch outputs. While one branch is aware of the inscribed surface, the other is aware of the extra region's borders or edges. The DARPA/NISTNimble Challenge 2016, the CASIA v1.0 Discovery I. Columbia Uncompressed dataset, the Carval hoSCI dataset, and the CASIAv0 dataset may all be used to train and test this network. This paper and the DARPA/NISTNimble Challenge 2016 include testing results for the data. DARPA/NISTNimble Challenge 2016 testing of this data. Training photos are divided into many patches in this work, which are then returned

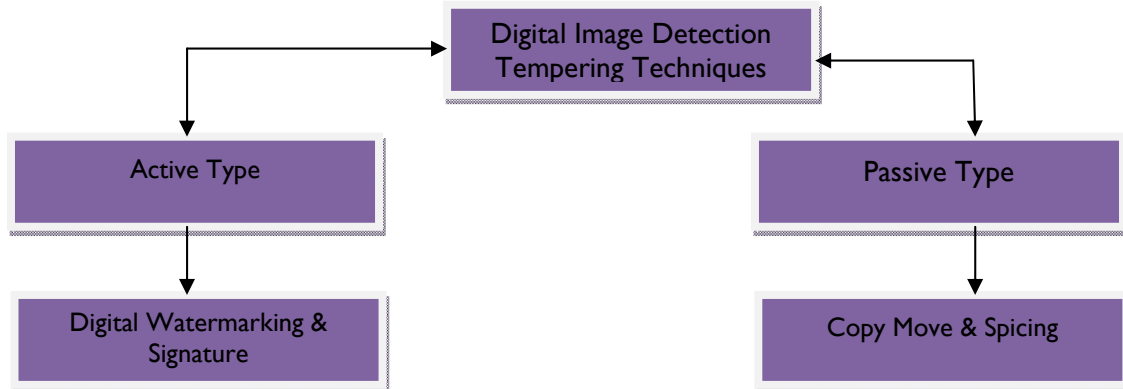


Fig4: Approaches for identifying manipulated image forgeries.

## VI. CONCLUSION

Considering the widespread problem of image tampering in daily life, the need for functional tampering detection algorithms that can perform various image forensic applications is increasing. This study discusses the art of fraud and the analysis of different types of fraud. The same simple concept of defining tattooed areas is clarified by showing the transition to various modifications. Future research should address these important issues by focusing on developing research methods that are flexible, high-fidelity, knowledge-based, and provide reliable solutions with minimal training and setback time. Our performance model for images created by artificial neural networks (GANs) differs from images using consumers of tware because GAN images are regenerated by the network neural system rather than changing pixel by pixel. No data is listed in this article for research purposes. Introduce a new architecture designed for finding altered images and partition in gartered areas. Achieve success in splitting and segmentingied images pyramid model with the Mutual ZPool2D module and meets or exceeds the base model in the database with different elements and controls. Updated face detection and overall image data using multiple control methods achieved over 90% accuracy, demonstrating the comprehensiveness and power of this model. Although this article does not discuss other attacks, it does show that the model can detect images on popular websites and Smartphone apps. These test results demonstrate the potential of the proposed method to spoof other means using images such as audio or text files. Modifications can be made to their applications to detect voice signals and languages. The next step is to figure out how the model works on images created by artificial neural networks which are different from images processed by consumer software.

## REFERENCES

1. Z.J.Barad,M.M.Goswami, Image Forgery Detection Using Deep Learning: A Survey,2020 6th International Conference on Advanced Computing and Communication Systems, ICACCS,2020, <https://doi.org/10.1109/ICACCS48705.2020.9074408.2020>.
2. J.Bunk,et al.,Detection and localization of image forgeries using resampling features and deep learning :IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops,2017, <https://doi.org/10.1109/CVPRW.2017.235>
3. O.E.David,N.S.Netanyahu, Deep Painter: painter classification using deep convolutional auto encoders, in: Lecture Notes in Computer Science ( Including Sub series Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics,2016, [https://doi.org/10.1007/978-3-319-44781-0\\_3](https://doi.org/10.1007/978-3-319-44781-0_3)
4. V.Dhir,A review on image forgery & its detection procedure,Int.J.Adv.Res.Comput.Sci.8(4)(2017).
5. A.Asaad,S.Jassim,Topological data analysis for image tampering detection, in: International Workshop on Digital Watermarking, Springer,Cham,2017,August,pp.136–146.
6. C.M.Hsu,J.C.Lee,W.K.Chen,An efficient detection algorithm for copy-move forgery, in: 2015 10th Asia Joint Conference on Information Security, IEEE, 2015,May,pp.33–36.
7. E.Ardizzone,A. Bruno, G. Mazzola, Copy–move forgery detection by matching triangles of keypoints, IEEE Trans. Inf.Forensics Secur.10(10)(2015)2084–2094.
8. S.Bayram,T.Sencar,N.Memon,An efficient and robust method for detecting copy-move forgery, in: Proceeding of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'09),2009,pp.1053–1056.Taipei,Taiwan.

9. T.Qazi,etal.,Survey on blind image forgery detection, IET Image Process.7(7) (2013),10.1109/it-ipr.2012.118.
10. M.Kumar,S.Srivastava,Image forgery detection based on physics and piXels:a study, Aust.J. Forensic Sci.(2019),<https://doi.org/10.1080/DOI50618.2017.1356868>.
11. A.K.Jaiswal, R.Srivastava, A technique for image splicing detection using hybrid feature set, Multimedia Tool. Appl. 79 (17–18) (2020), <https://doi.org/10.1007/s11042-019-08480-6>.
12. L.Bondi,S.Lameri, D. Guera, P.Bestagini, E.J. Delp, S. Tubaro,Tampering detection and localization through clustering of camera-based CNN features, in: In CVPR Workshops vol.2,2017,July.
13. D.Cozzolino,L.Verdoliva,Single-image splicing localization through auto encoder-based anomaly detection,: In the 2016 IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, 2016,December,pp.1–6
14. Micklethwaite.(2020) Zombiebomb shelliran's zombiea ngelinajolie's a photo shop fraud, pics show as she's seen for first time inyears.[Online].Available: <https://www.thesun.co.uk/news/13507987/iran-zombie-angelina-jolie-photoshop-fraud-pics/>
15. Connexion france.com.(2021)Eu's health pass aims to crack down on fake covid certificates.[Online].Available: <https://www.connexionfrance.com/French-news/EU-s-health-pass-aims-to-crack-down-on-fake-Covid-certificates>
16. O.SeddiquandS.Sheth.(2021)Trump lawyer accuses house managers of manipulating evidence by pointing to doctored tweets that weren't used in the impeachment trial.[Online].Available: <https://www.businessinsider.com/trump-lawyer-accuses-house-managers-of-manipulating-evidence-2021-2>
17. D.Low.(2021)\$4,000 fine for nus drop out who forged degree certificate to get part-time teaching job.[Online].Available: <https://www.straitstimes.com/singapore/courts-crime/4000-fine-for-ex-nus-student-who-forged-degree-certificate-to-get-part-time>
18. T.Lince.(2021)Bribery, impersonation, abuse: shocking details revealed in pakistan fraud case that targeted usptousers world trade mark review.[Online].Available: <https://www.worldtrademarkreview.com/enforcement-and-litigation/bribery-impersonation-abuse-shocking-details-revealed-in-pakistan-fraud-case-targeted-uspto-users>
19. A.C.Popescu and H. Farid, Exposing digital forgeries in color filter array interpolated images, IEEE Transactions on Signal Processing, vol. 53,no. 10,pp. 3948–3959,2005.
20. D.Y.HsiaoandS.C.Pei,Detecting digital tampering by blur estimation, in First International Work shop on Systematic Approaches to Digital Forensic Engineering (SADFE'05). IEEE, 2005,pp. 264–278.
21. J.He,Z.Lin,L.Wang,andX.Tang,Detecting doctored jpeg images via dct coefficient analysis,II in European conference on computer vision. Springer,2006, pp.423–435.
22. E.KeeandH.Farid, Exposing digital forgeries from 3-d lighting environments, in 2010 IEEE International Workshop on Information Forensics and Security. IEEE, 2010,pp. 1–6.
23. B.Peng,W.Wang,J.Dong,and T.Tan, Optimized 3d lighting environment estimation for image forgery detection, IEEE Transactions on Information Forensics and Security, vol. 12,no. 2, pp.479–494, 2016.
24. C.Chen,S.McCloskey,and J.Yu, Image splicing detection via camera response function analysis, In Proceedings of the IEEE conference on computer vision and pattern recognition, 2017,pp. 5087–5096.
25. H.Li,W.Luo,X.Qiu,andJ.Huang, Image forgery localization via integrating tampering possibility maps, IEEE Transactions on Information Forensics and Security,vol.12,no.5, pp. 1240–1252,2017.